Notice of Allowability	Application No.	Applicant(s)	
	10/036,521	ACKROYD, ROBERT JOHN	
	Examiner	Art Unit	
	Eleni A. Shiferaw	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *03/20/2007*.

2. ☒ The allowed claim(s) is/are *1,3-10,12-19,21-27 and 30-34*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

5/27/07

DETAILED ACTION

1. Examiner initiated interview has been made on May 25, 2007, to move dependent claims to base claims to particularly point out the invention and clarify claims languages, with Kevin J. Zilka. Based on the interview examiner's amendment has been made to independent claims 1, 10 and 19 to include limitation of dependent claims 2, 11, and 20, dependent claims 2, 11, and 20 are canceled, and dependent claims 3, 5, 12, 14, 21, and 23 are amended to correct dependency on cancelled claims.

EXAMINER'S AMENDMENT

2. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Kevin J. Zilka on May 24, 2007.

3. Independent claims 1, 10 and 19 are amended to include limitation of claims 2, 11, and 20, dependent claims 2, 11, and 20 are canceled, and dependent claims 3, 5, 12, 14, 21, and 23 are amended to correct dependency on cancelled claims as follows.

1. (Currently Amended) A program stored on a computer-readable medium for controlling a managing computer to manage malware protection within a computer

network containing a plurality of network connected computers, said computer program product comprising:

receiving code for receiving at said managing computer a plurality of log data messages identifying detection of malware by respective ones of said plurality of network connected computers;

detecting code for detecting from said plurality of log data messages received by said managing computer a pattern and a network-wide threshold of malware detection across said plurality of network connected computers matching at least one predetermined trigger, the network-wide threshold being applied to a sum of detections, the detections each being associated with a different one: of the: network connected computers; ~~and~~

wherein said plurality of network connected computers each have a malware scanner for scanning computer files to detect malware within said computer files;

action performing code, responsive to detection of one of said at least one predetermined trigger to perform at least one predetermined anti-malware action;

wherein predefined network-wide thresholds and patterns are provided as templates; and

wherein the predefined network-wide thresholds and patterns are customized ~~to particular circumstances.~~ based on the network being protected.

2. (Canceled)

3. (Currently Amended) A program stored on a. computer-readable medium as claimed in claim ~~2~~ 1, wherein said malware scanner includes malware definition data for identifying malware to be detected.

5. (Currently Amended) A program stored on a computer-readable medium as claimed in claim ~~2~~ 1, wherein said at least one predetermined anti-malware action includes altering at least one scanner setting of at least one of said malware scanners such that said at least one of said malware scanners performs more thorough malware scanning.

10. (Currently Amended) A method of managing malware protection within a computer network containing a plurality of network connected computers, said method comprising the steps of:

receiving at a managing computer a plurality of log data messages identifying detection of malware by respective ones of said plurality of network connected computers;

detecting from said plurality of log data messages received by said managing computer a pattern and a network-wide threshold of malware detection across said plurality of network connected computers matching at least one predetermined trigger, the network-wide threshold being applied to a sum of detections, the detections each being associated with a different one of the network connected computers; ~~and~~

wherein said plurality of network connected computers each have a malware scanner that serves to scan computer files to detected malware within said computer files;

in response to detection of said at least one predetermined trigger, performing at least one predetermined anti-malware action;

wherein predefined network-wide thresholds and patterns are provided as templates; and

wherein the predefined network-wide thresholds and patterns are customized ~~to particular circumstances.~~ based on the network being protected.

11. (Canceled)

12. (Currently Amended) A method as claimed in claim ~~11~~ 10, wherein said malware scanner uses malware definition data to identify malware to be detected.

14. (Currently Amended) A method as claimed in claim ~~11~~ 10, wherein said at least one predetermined anti-malware action includes altering at least one scanner setting of at least one malware scanner such that said malware scanner performs more thorough malware scanning.

19. (Currently Amended) Apparatus for managing malware protection within a computer network said computer network said computer network containing a plurality of network connected computers, said apparatus comprising:

receiving logic for receiving at a managing computer a plurality of log data messages identifying detection of malware by respective ones of said plurality of network connected computers;

detecting logic for detecting from said plurality of log data messages received by said managing computer a pattern and a network-wide threshold of malware detection across said plurality of network connected computers matching at least one predetermined trigger, the network-wide threshold being applied to a sum of detections, the detections each being associated with a different one of the network connected computers; ~~and~~

wherein each of said plurality of network connected computers have a malware scanner that serves to scan computer files to detected malware within said computer files;

action performing logic, in response to detection of at least one predetermined trigger, for performing at least one predetermined anti-malware action;

wherein predefined network-wide thresholds and patters are provided as templates; and

wherein the predefined network-wide thresholds and patterns are customized ~~to particular circumstances.~~ based on the network being protected.

20. (Canceled)

21. (Currently Amended) Apparatus as claimed in claim ~~20~~ 19, wherein said malware includes malware definition data to identify malware to be detected.

23. (Currently Amended) Apparatus as claimed in claim ~~20~~ 19, wherein at least one predetermined anti-malware action includes altering at least one scanner setting of at least one malware scanner such that said malware scanner performs more thorough malware scanning.

28. (Canceled)

29. (Canceled)

Response to Arguments

4. Applicant's arguments filed on 03/20/2007 are persuasive.

Allowable Subject Matter

5. Claims 1, 3-10, 12-19, 21-27, and 30-34 are allowed.

The following is a statement of reasons for the indication of allowable subject matter: The applied arts and/or prior art of record alone or in combination fail to disclose wherein plurality of network connected computers each having a malware scanner for scanning computer files to detect malware within said computer and transmitting plurality log data messages, if malware detected, to managing computer via a network and the managing computer detecting from a plurality of log data messages a pattern and a network-wide threshold of malware detection across said plurality of network connected computers matching at least one predetermined trigger, the network-wide threshold being applied to a sum of detections, the detections each being associated with a different one of the network connected computers, and performing action.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for

Allowance."

Conclusion

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A. Shiferaw whose telephone number is 571-272-3867. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser R. Moazzami can be reached on (571) 272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

EAS

May 25, 2007

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

5/27/07